





Presentation to the SSCA 2015 Fall Forum

Business Due Diligence Information - Risk Indicators, FY16 activities, projected IOC

Angela Smith & Rowan Ha
Cybersecurity & Resilience
Office of Government-wide Policy
September 2, 2015

Agenda



-  Brief Overview of BDDIS
-  Risk Indicators
-  FY2016 Plans
-  Projected Roadmap to IOC

Overview of BDDIS

- What is it?
- Why do we need it?
- How will it work?

WHAT IS IT?

- Central government-wide service/solution that enables agencies to perform substantially improved “business due diligence” for ICT acquisitions.
- Provides capability to research, collect, assess, and share risk indicator data about a particular vendor, product, and/or service
- The BDDIS will store, maintain, and provide access to a central (government-wide) repository of risk information

HOW WILL IT WORK?

1. BUYER:

- Risk Tolerance – relative to importance of Risk Categories
- Seller and Deliverable

2. SELLER (VOLUNTARY):

- Information about the Seller related to Risk Categories
- From the Seller

3. "BIG DATA:"

- Information about the Seller related to Risk Categories
- From "Big Data"

DATA & INFORMATION INPUTS

FUNCTIONS & OUTPUTS

Initial Automated Risk Score

- Dashboard view
- Comparison of Seller and "Big Data" inputs to Buyer's Risk Tolerance

Aggregate Multiple Data Sources

- Data supporting risk score
- Authoritative and secondary source information

Perform Analytics

- Compare Seller inputs with "Big Data" inputs
- Identify correlations

Conduct In-depth Investigations (as needed)

- On-site inspections
- Process reviews
- Personnel interviews

WHY DO WE NEED IT?

DRIVERS & INFLUENCES – CYBERSECURITY IS URGENT PRIORITY

- Administration & Congressional **Priority** – e.g., Cyber CAP Goal, New Cyber Laws, Cybersprint, PPD-21; EO 13636
- High-profile **Breaches** & Ever-increasing **Threat**
Need to **Improve** Cyber Protections in **Acquisitions**
- **Inadequate Access** to Due Diligence Data
- **Risk Management** Framework
- Private Sector & Insurance Industry - **Alignment** of Need & Approach

STAKEHOLDER & CUSTOMER OUTREACH – CONFIRMATION OF NEED

- Issued **RFI** – received + 30 Responses
- Extensive **Outreach & Engagement**: Qtly Software & Supply Chain Assurance Forum; RSA Conference; Open Group Forum; Defense Science Board Brief; Exostar; Cybersecurity Law Institute & Agencies (TSA, DoD ATL; State, Treasury, DHS, FBI, SSA, DoE, NASA, DNI + others)
- **Federal Register** Notice and Comments
- Interact & GSA.gov **web content**

GSA Office of Government-wide Policy - Cybersecurity & Resilience

We need to establish a
baseline set of risk indicators

We need your input!

RISK INDICATORS

- List compiled of categories and subcategories of data/information for use in conducting business due diligence
- Current list is based on research conducted and input received from RFIs, BDD pilot results, stakeholder engagements
- Planned next step: Publish notice in Federal Register for public comment
- We welcome your review, comments, suggested changes, and/or validation of the categories, indicators, groupings, and definitions

RISK INDICATORS

People

Company leadership, ownership, management, mergers and acquisitions activity, media activity, organizational reputation, and personnel associations; Foreign ownership, control or influence of contractor or its suppliers; Insider Threat and physical security practices

Processes

Organization's financial health, including access to and sources of funding, solvency, and liquidity; Record of integrity and business ethics, including but not limited to legal and regulatory issues; Cybersecurity practices, including but not limited to network defense, incident response, information security practices, and participation in Information Sharing and Analysis Organizations; Financial systems, purchasing systems, production control procedures, property control systems, quality assurance measures, safety programs, insurance, physical security practices, insider threat practices; Existing commercial and gov't clients/customers, small business subcontracting and diversity programs, cost performance (over/under -runs), delivery performance, customer service practices

RISK INDICATORS

Technology

Product and component manufacturing practices including supply chains, production, construction, and technical equipment and facilities, and logistics , physical security requirements, and reseller and supplier qualification requirements, controls, business requirements, and enforcement mechanisms; Hardware and software assurance practices, anti-counterfeit, intellectual property, and product and service testing policies and procedures



Certification/ Conformance

Indicators: (1st, 2nd or 3rd party) with U.S. Federal government or consensus-based market standards, including, but not limited to: Cost Accounting Standards, Facility and Personnel security clearances, FedRAMP, FIPS (ATO), CTPAT, ISO, SAE, COBIT, Open Group OTTP-S.

RISK INDICATORS

People Indicators Definitions

Principal	A person(s) having primary management or supervisory responsibilities within a business entity (e.g., general manager; plant manager; head of a division or business segment; and similar positions).
Highest-level Owner	The entity that owns or controls an immediate owner of the offeror, or that owns or controls one or more entities that control an immediate owner of the offeror. No entity owns or exercises control of the highest level owner.
Immediate owner	An entity, other than the offeror, that has direct control of the offeror. Indicators of control include, but are not limited to, one or more of the following: ownership or interlocking management, identity of interests among family members, shared facilities and equipment, and the common use of employees.
★ Organizational Reputation	Observers collective judgments of a corporation based on assessments of financial, social and environmental impacts attributed to the corporation over time.
Affiliates	Organizations or individuals who are directly or indirectly, (1) either one controls or has the power to control the other, or (2) a third party controls or has the power to control both....
Foreign Ownership	Etc etc
Insider Threat	

FY2016 PLANS

- Finalize Risk Indicators
- GSA-NIST Predictive Analytics Project
- Pilot Extension – Assess top 50 GSA ICT vendors
- Create and Prototype Government-wide ConOps
- Validate Correlation of Risk Indicators to Desired Performance Levels
- Finalize Core Capabilities (IOC) Requirements

IOC/FOC Timeline

DEVELOP/PROTOTYPE ConOps (FY2016)

- UMD-NIST Predictive Analytics Project
- Extend Pilot – Assess top 50 GSA ICT vendors
- Baseline Risk Indicators/Definitions
- ConOps Document & Prototype ConOps
- Finalize Requirements

BUILD OUT INITIAL OPERATIONAL CAPABILITY (FY2017)

- Transition Plan to Scale for Government-wide Use
- Execute Plan to Achieve Initial Operational Capability (IOC)

FINAL OPERATIONAL CAPABILITY (FY2018 +)

- Enhance/Evolve BDDIS Solution

Any Questions??

The proposed risk indicators & definitions will be posted on GSA's SSCA Interact site (
<https://interact.gsa.gov/group/software-and-supply-chain-assurance-ssca-forum-wg>). In addition, GSA will provide guidance about where, when, and how to submit your comments.

All comments received will be compiled and anonymized as "SSCA Forum Participant" comments